日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月２８日

出願番号
Application Number: 特願２００３－０５３３６２

[ST. 10/C]: ［ＪＰ２００３－０５３３６２］

出願人
Applicant(s): 松下電器産業株式会社

２００４年　１月１４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１１１５１３

【書類名】　特許願
【整理番号】　2030750003
【提出日】　平成15年 2月28日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　峰村　淳
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100099254
　【弁理士】
　【氏名又は名称】　役　昌明
【選任した代理人】
　【識別番号】　100100918
　【弁理士】
　【氏名又は名称】　大橋　公治
【選任した代理人】
　【識別番号】　100105485
　【弁理士】
　【氏名又は名称】　平野　雅典
【選任した代理人】
　【識別番号】　100108729
　【弁理士】
　【氏名又は名称】　林　紘樹

【手数料の表示】

【予納台帳番号】　037419

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9102150

【包括委任状番号】　9116348

【包括委任状番号】　9600935

【包括委任状番号】　9700485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アプリケーション認証システムと装置

【特許請求の範囲】

【請求項１】　安全な情報秘匿領域を持たない端末に固定的にまたは着脱可能に接続されたセキュアデバイスが、前記端末に格納されたアプリケーションを認証するアプリケーション認証システムであって、

セキュアデバイスは、端末上のアプリケーション実行手段を認証し、前記アプリケーション実行手段の、セキュアデバイスへのアクセスを要求するアプリケーションに関する処理に基づいて、前記アプリケーションを認証することを特徴とするアプリケーション認証システム。

【請求項２】　前記アプリケーション実行手段は、電子署名が付された前記アプリケーションのダイジェストデータを算出して、前記ダイジェストデータと前記電子署名とをセキュアデバイスに提示し、セキュアデバイスは、提示されたダイジェストデータを用いて前記電子署名を検証し、検証結果が正常であるとき、前記アプリケーションを認証することを特徴とする請求項１に記載のアプリケーション認証システム。

【請求項３】　前記アプリケーション実行手段は、前記アプリケーションのダイジェストデータを算出して、前記ダイジェストデータをセキュアデバイスに提示し、セキュアデバイスは、提示されたダイジェストデータを自ら保持するダイジェストデータと照合し、照合結果が正常であるとき、前記アプリケーションを認証することを特徴とする請求項１に記載のアプリケーション認証システム。

【請求項４】　前記アプリケーション実行手段は、前記アプリケーションのダイジェストデータを算出した後、セキュアデバイスに対して処理要求命令を送出し、セキュアデバイスは、第一の情報をアプリケーション実行手段へ送出し、アプリケーション実行手段は、前記第一の情報を前記ダイジェストデータで暗号化してセキュアデバイスに送出し、セキュアデバイスは、前記暗号化された情報を自ら保持するダイジェストデータで復号し、復号によって得られる情報と前記第一の情報とを照合することを特徴とする請求項３に記載のアプリケーション認証システム。

【請求項５】　前記アプリケーション実行手段は、電子署名が付された前記アプリケーションの前記電子署名を検証して前記アプリケーションを認証し、セキュアデバイスは、前記アプリケーション実行手段の認証結果を受け入れて前記アプリケーションを認証することを特徴とする請求項１に記載のアプリケーション認証システム。

【請求項６】　セキュアデバイスが前記アプリケーション実行手段を認証した際に、セキュアデバイスと前記アプリケーション実行手段とで第二の情報を共有し、セキュアデバイスは、セキュアデバイスが認証したアプリケーションからの処理要求に前記第二の情報が加味されている場合に、その処理要求を受け付けることを特徴とする請求項２から５のいずれかに記載のアプリケーション認証システム。

【請求項７】　端末に固定的にまたは着脱可能に接続されたデバイスであって、前記端末を認証する処理を行うカードマネージャと、前記端末に格納された、アクセスを要求するアプリケーションに対して認証処理を行うカードアプリケーションとを備え、前記カードアプリケーションは、前記端末が前記アプリケーションに対して行った処理に基づいて前記アプリケーションを認証し、前記カードマネージャの前記端末を認証する処理が完了していることを確認して、認証した前記アプリケーションのアクセス要求を受け付けることを特徴とするセキュアデバイス。

【請求項８】　アプリケーション実行手段と、アプリケーションとを備え、前記アプリケーション実行手段は、装着されたセキュアデバイスが前記アプリケーション実行手段を認証した後、セキュアデバイスへのアクセスを要求する前記アプリケーションのダイジェストデータを算出し、前記ダイジェストデータを用いて前記アプリケーションを認証した後、前記セキュアデバイスにアクセス要求を行うことを特徴とする端末。

【請求項９】　前記アプリケーション実行手段は、前記ダイジェストデータを用いて前記アプリケーションに付された電子署名を検証し、前記アプリケーションを認証することを特徴とする請求項８に記載の端末。

【請求項１０】　前記アプリケーション実行手段は、前記ダイジェストデー

タを前記セキュアデバイスに送り、前記セキュアデバイスから前記ダイジェストデータの照合結果を取得して、前記アプリケーションを認証することを特徴とする請求項８に記載の端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＣカードなどのセキュアデバイス上で動作するカードアプリケーションが、携帯端末などの端末上で動作するアプリケーションを認証するアプリケーション認証システムと、そのセキュアデバイスと端末に関し、特に、端末上のアプリケーションがセキュアデバイスを利用する際に必要となる認証処理を実現するものである。

【０００２】

【従来の技術】

近年、情報をセキュアに格納することが可能なＩＣカードなどのセキュアデバイスは、電子商取引や入退出管理、定期券など、多方面で利用されており、今後、携帯端末などのモバイル機能を活用して、その利用範囲は、益々広がるものと見られている。

【０００３】

図８には、携帯端末３０上で動作するアプリケーション（以下、省略して「アプリ」と言う）が、セキュアデバイス１０に格納されたセキュアなデータを利用して実行可能となると見られているサービスの数々を模式的に示している。

セキュアデバイス内で動作するアプリ（カードアプリ）は、下記非特許文献１に記載されているように、Java(登録商標)などのプログラミング言語で作成されてセキュアデバイスに搭載される。カードアプリは、セキュアデバイスに格納したセキュアなデータの利用を求める外部アプリに対して、認証を行い、安全性を確認してから、外部アプリのコマンドを受け付ける。

【０００４】

【非特許文献１】

「Ｉｎｔｅｒｆａｃｅ」２００３年３月号、ＣＱ出版社、ｐ．８２～９０

【０００５】

【発明が解決しようとする課題】

しかし、従来のセキュアデバイスは、携帯端末にダウンロードされたアプリに対する認証手段を有しておらず、そのため、携帯端末にダウンロードされたアプリは、セキュアデバイスに格納されたデータを利用することができない。

これは、次のような事情に拠る。

通常、認証処理では、当人しか知り得ない情報を知っているかどうかを確認し、知っている場合に、当人と認める。図９は、この方式による相互認証をセキュアデバイス１０のカードアプリ１１と、携帯端末３０の端末アプリ（ここではJava(登録商標)言語で記述されたJava(登録商標)アプリとする）３１とに当て嵌めたときの様子を模式的に示している。機密データの保管機能を持つセキュアデバイス１０は、ハードウエア的に安全に作られた耐タンパ性の領域に秘密の情報（暗号鍵など）を保持することができる。一方、携帯端末３０が秘密情報を扱うには、セキュリティが要求されるため、領域３１全体が耐タンパ性であるか、秘密情報を保持する耐タンパ性の領域３５が在って、領域３１が領域３５に認証されている必要がある。こうした状況にあれば、カードアプリ１１と、携帯端末３０のＯＳ（あるいはＶＭ（virtual machine））３２の制御の下で動作するJava(登録商標)アプリ３１とが情報を交換し、互いに共通の秘密情報を保持していることが確認できれば、相互認証は成立する。

【０００６】

しかし、実際には、携帯端末３０は、秘密情報を安全に保持できる領域を有していない。そのため、カードアプリ１１は、共通の秘密情報を用いて相手認証を行うことができず、従って、携帯端末３０にダウンロードされたJava(登録商標)アプリ３１は、これまで、セキュアデバイス１０に格納されたデータを利用することができなかった。

こうした事情から、携帯端末３０にセキュアデバイス１０を装着して、ネットワークを通じてサービスサーバからサービスを受ける場合でも、これまでは、セキュアデバイス１０と相互認証したサービスサーバは、セキュアデバイス１０に格納されたデータを利用できるが、携帯端末３０は、データをスルーする土管の

役割しか果たすことができなかった。そのため、図８に示すように、携帯端末３０のアプリがセキュアデバイス１０のデータを読み／書きして、計算や表示などの高度の処理を行うシステムは実現することができなかった。

【０００７】

本発明は、こうした従来の問題点を解決するものであり、安全な情報秘匿領域を持たない端末上のアプリに対するセキュアデバイスの認証が可能なアプリケーション認証システムを提供し、そのシステムを構成するセキュアデバイス及び端末を提供することを目的としている。

【０００８】

【課題を解決するための手段】

そこで、本発明では、安全な情報秘匿領域を持たない端末に固定的にまたは着脱可能に接続されたセキュアデバイスが、前記端末に格納されたアプリを認証するアプリケーション認証システムにおいて、セキュアデバイスが、端末上のアプリ実行手段を認証し、このアプリ実行手段の、セキュアデバイスへのアクセスを要求するアプリに関する処理に基づいて、アプリを認証するように構成している。

【０００９】

また、本発明では、端末に固定的にまたは着脱可能に接続されるセキュアデバイスに、端末を認証する処理を行うカードマネージャと、端末に格納された、アクセスを要求するアプリに対して認証処理を行うカードアプリケーションとを設け、カードアプリケーションは、端末がアプリに対して行った処理に基づいてアプリを認証し、カードマネージャの前記端末を認証する処理が完了していることを確認して、認証したアプリのアクセス要求を受け付けるように構成している。

【００１０】

また、本発明では、アプリ実行手段と、アプリとを備える端末において、アプリ実行手段は、装着されたセキュアデバイスがアプリ実行手段を認証する処理の完了後、セキュアデバイスへのアクセスを要求するアプリのダイジェストデータを算出し、このダイジェストデータを用いてアプリを認証した後、セキュアデバイスにアクセス要求を行うように構成している。

【００１１】

そのため、セキュアデバイスの端末認証、及び、端末内でのアプリの認証とを結び付けることで、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。

【００１２】

【発明の実施の形態】

（第１の実施形態）

本発明の第１の実施形態におけるアプリケーション認証システムでは、携帯端末上で動作する端末アプリを認証するため、セキュアデバイスのカードアプリは、端末アプリが正規のアプリであるか否かを確認する。カードアプリは、端末アプリが正規のアプリと確認できたとき、認証処理が正常に終了したものとして、端末アプリのアクセス要求を受け付ける。

【００１３】

図２は、このシステムを構成するセキュアデバイス１０と携帯端末３０とを模式的に示している。携帯端末３０は、工場出荷時に情報がＲＯＭやフラッシュメモリに書き込まれ、以後、情報の書き換えができない「書き換え不可領域３０２」と、ダウンロードされたアプリが書き込まれる「ユーザ書き換え領域３０１」とを備えており、ユーザ書き換え領域３０１には、電子署名３４が付されたJava(登録商標)アプリ３１が格納され、また、書き換え不可領域３０２には、ＯＳ３２や、Java(登録商標)言語で記述されたプログラムを実行するためのJava(登録商標)実行環境（ＪＡＭ）３３が格納されている。

【００１４】

なお、「書き換え不可領域３０２」は、端末上の操作（例えば、アプリケーション３１）や、外部（例えば、カード１０）からのアクセスなどにより、そこに格納された情報が書き換えられることがない領域を意味し、その領域自身が物理的書き換え不可能な仕組み（例えばＲＯＭ）を有しているか否かは問わない。

【００１５】

Java(登録商標)アプリ３１の電子署名３４は、Java(登録商標)アプリ３１の正当性を証明する認証局によって付されており、Java(登録商標)アプリ３１のデー

タにハッシュ演算を行ってダイジェストデータを生成し、このダイジェストデータを認証局の秘密鍵で暗号化して生成されている。

また、ＪＡＭ３３には、携帯端末３０がセキュアデバイス１０との相互認証に用いる端末認証情報と、電子署名３４の検証用公開鍵を含む認証局のアプリ証明書とが入力される（ここで「入力される」とは、それぞれの情報が、コードとしてＪＡＭ３３に埋め込まれたり、必要なときにファイルとして取得可能であることを意味する）。

【００１６】

一方、セキュアデバイス１０は、携帯端末３０に対する認証処理を行う共通ライブラリ（カードマネージャ）１３と、携帯端末３０で動作するJava(登録商標)アプリ３１の認証処理を行うカードアプリ１１と、認証局の公開鍵を証明する署名検証用ルート証明書１４とを備えている。

【００１７】

また、カードマネージャ１３には、セキュアデバイス１０が携帯端末３０との相互認証に用いる端末認証情報が入力される（ここで「入力される」とは、それぞれの情報が、コードとしてカードマネージャ１３に埋め込まれたり、必要なときにファイルとして取得可能であることを意味する）。

【００１８】

なお、本発明では、セキュアデバイス１０が携帯端末３０を認証することは必要であるが、携帯端末３０がセキュアデバイス１０を認証することは必ずしも必要ではない。各実施形態では、セキュアデバイス１０と携帯端末３０とが「相互認証」する場合について示しているが、相互認証は必須では無く、セキュアデバイス１０が携帯端末３０を認証する「片側認証」で良い。

【００１９】

図１には、このシステムにおいて、セキュアデバイス１０のカードアプリ１１が、携帯端末３０で動作するJava(登録商標)アプリ３１を認証するまでの手順を矢印で示している。

セキュアデバイス１０が携帯端末３０に装着されると、セキュアデバイス１０のカードマネージャ１３は、携帯端末３０のＪＡＭ３３との間で、それぞれの端

末認証情報を用いて、装置間の相互認証処理を行う（１）。相互認証に成功すると、カードマネージャ１３は、その成功を示すフラグ（相互認証パスフラグ）をセキュアデバイス１０内に立てる。

【００２０】

なお、セキュアデバイスによる端末の認証方式については、種々のものが知られており、このシステムでも、それらの方式を用いることができる。例えば、ＴＣＰＡ（Trusted Computing Platform Alliance）の方式を用いて、セキュアデバイスがＢＩＯＳ（Basic Input Output System）を認証後、ＢＩＯＳがＯＳを認証し、次に、ＯＳがJava(登録商標)実行環境を認証するようにしてもよい。また、耐タンパ性のＳＩＭカードやセキュアＬＳＩを持つ携帯端末の場合には、チャレンジ＆レスポンス（challenge＆response）方式を用いることができる。要は、正規端末であることの認証が出来れば良く、特定機器へのバインド方式であっても一向構わない。

【００２１】

携帯端末３０のＪＡＭ３３は、セキュアデバイス１０との相互認証に成功すると、セキュアデバイス１０へのアクセス機能を開始し、Java(登録商標)アプリ３１は、ＪＡＭ３３に対してセキュアデバイス１０へのアクセスを要求する（２－１）。この要求を受けたＪＡＭ３３は、アプリ証明書に含まれる公開鍵を用いてJava(登録商標)アプリ３１の電子署名３４を検証し、それによりJava(登録商標)アプリ３１を認証する（２－２）。

【００２２】

電子署名３４の検証は、Java(登録商標)アプリ３１のデータにハッシュ演算を行ってダイジェストデータを生成し、このダイジェストデータと、電子署名３４を公開鍵で復号化したデータとを比較することによって行われる。それらが一致する場合には、ＪＡＭ３３は、Java(登録商標)アプリ３１の正当性を認証し、データが改ざんされていないことを確認することができる。

【００２３】

Java(登録商標)アプリ３１を認証したＪＡＭ３３は、生成したダイジェストデータと、Java(登録商標)アプリ３１の電子署名３４とをセキュアデバイス１０の

カードアプリ１１に提示する（２－３）。これを受けて、カードアプリ１１は、署名検証用ルート証明書１４から得た公開鍵を用いて電子署名３４を復号化し、ＪＡＭ３３から送られたダイジェストデータとの一致を検証する。

Java(登録商標)アプリ３１を認証したＪＡＭ３３は、Java(登録商標)アプリ３１からのアクセス要求を実行し、カードアプリ１１にコマンドを送信する（３）。ダイジェストデータの検証に成功したカードアプリ１１は、カードマネージャ１３による機器認証が完了していることを相互認証パスフラグで確認した後、このコマンドを受け付ける。

【００２４】

このように、このアプリケーション認証システムのセキュアデバイスは、携帯端末で動作するアプリが正規のものであることを確認することで、そのアプリを認証する。そして、この確認を行うため、第１段階では、携帯端末を認証することにより、携帯端末の書き換え不可領域に格納されたJava(登録商標)実行環境（アプリ実行手段）の正当性を確認する。この確認が一度得られれば、アプリ実行手段の書き換えは不可能であるため、アプリ実行手段に対する信頼性は、その後も継続することとなる。

【００２５】

第２段階では、携帯端末の中でセキュアデバイスの信頼性を得たアプリ実行手段が、電子署名付きのアプリを認証し、このアプリのダイジェストデータと電子署名とをセキュアデバイスに渡す。

セキュアデバイスは、信頼を置くアプリ実行手段から、生成直後に渡されたダイジェストデータを信頼に足るものと見て、第３段階では、このダイジェストデータを電子署名によって検証する。

【００２６】

この検証結果が正常である場合、セキュアデバイスは、第１段階、第２段階、及び、第３段階の認証処理に基づいて、端末で動作するアプリが正規のアプリであると確認することができる。

このように、このアプリケーション認証システムでは、第１段階、第２段階、及び、第３段階の認証処理の連鎖により、セキュアデバイスが、安全な情報秘匿

領域を持たない端末上のアプリに対して認証することを可能にしている。

【００２７】

（第２の実施形態）

本発明の第２の実施形態では、アプリを特定するための認証情報が格納されて発行されるセキュアデバイスと、そのアプリが動作する携帯端末とから成るアプリケーション認証システムについて説明する。

このセキュアデバイスは、携帯端末にダウンロードされるアプリと組になってサービスを実現するために作成されており、例えば、図８に示す「電子チケットアプリ」が携帯端末３０にダウンロードされる場合では、セキュアデバイス１０は、電子チケット用のセキュアデバイスと言うことになる。

【００２８】

図４は、このシステムを構成するセキュアデバイス１０と携帯端末３０とを模式的に示している。携帯端末３０のユーザ書き換え領域３０１に格納されているJava(登録商標)アプリ３１は、署名を有していない。そのため、ＪＡＭ３３へのアプリ証明書の入力は無い。また、セキュアデバイス１０には、Java(登録商標)アプリ３１を特定するためのダイジェストデータ１５などのアプリ認証情報が予め格納されている。その他の構成は、第１の実施形態と変わりが無い。

【００２９】

図３には、このシステムにおける認証手順を矢印で示している。

セキュアデバイス１０が携帯端末３０に装着されると、第１の実施形態（図１）と同様に、セキュアデバイス１０のカードマネージャ１３と、携帯端末３０のＪＡＭ３３との間で、装置間の相互認証処理が行われ（１）、相互認証に成功すると、カードマネージャ１３は、その成功を示す相互認証パスフラグをセキュアデバイス１０内に立てる。また、携帯端末３０のＪＡＭ３３は、セキュアデバイス１０との相互認証に成功すると、セキュアデバイス１０へのアクセス機能を開始し、Java(登録商標)アプリ３１は、ＪＡＭ３３に対してセキュアデバイス１０へのアクセスを要求する（２－１）。

【００３０】

この要求を受けたＪＡＭ３３は、Java(登録商標)アプリ３１のデータにハッシ

ュ演算を行ってダイジェストデータを生成し（２－２）、このダイジェストデータをセキュアデバイス１０のカードアプリ１１に提示する（２－３）。カードアプリ１１は、相互認証パスフラグを参照して、カードマネージャ１３による機器認証が完了していることを確認した後、ＪＡＭ３３から提示されたダイジェストデータと、セキュアデバイス１０内で密かに保持されているダイジェストデータ１５とを照合し、認証結果をＪＡＭ３３に返す（２－４）。Java(登録商標)アプリ３１が認証されたことを知ったＪＡＭ３３は、Java(登録商標)アプリ３１からのアクセス要求を実行し、カードアプリ１１にコマンドを送信する（３）。

【００３１】

このように、このアプリケーション認証システムでは、アプリに対する電子署名が不要（勿論、有っても構わない）であり、システムを簡略化できる。

また、オペレータがアプリに署名を付けるシステムでは、オペレータによる統制を排除できないが、アプリに対する電子署名が不要なこのシステムでは、オペレータの影響を受けずにビジネスを展開することができ、アプリのダウンロードが可能な体制を整えた上で、アプリの認証情報を埋め込んだセキュアデバイスをユーザに配布すれば、直ぐにサービスを開始することができる。

【００３２】

なお、アプリ実行手段からセキュアデバイスへのアプリケーション認証のためのデータ（ダイジェストデータ）の提示処理である処理（２－３）のより具体的な方法としては、次のようなものが考えられる。例えば、ＰＩＮの照合などを行うときに使用する既存のコマンドのＶｅｒｉｆｙを使用して、ＰＩＮの替わりにアプリ認証用のデータを提示する手法や、ＩＣカードの外部認証で使用するchallenge&responce方式用の既存のコマンドである GetChallenge と ExternalAuthenticate において、秘密鍵の替わりにアプリ認証用のデータを使用して、データを提示する手法などである。

【００３３】

後者の場合、通常のchallenge-response方式では、機器Ｂが機器Ａを認証する場合、機器Ａから機器Ｂに対してchallenge-response処理のトリガにあたるGetChallengeを送信すると、機器Ｂにて、あらかじめ保持されている情報や任意に

生成される情報（乱数など）である第一の情報を機器Ａに返信して、機器Ａにて前記第一の情報をあらかじめ保持している秘密鍵（秘密情報Ａ）などで暗号化した上で機器Ａに送信し（ExternalAutheticate）、機器Ｂにて暗号化された情報をあらかじめ保持している秘密鍵（秘密情報Ｂ：秘密情報Ａに対応した秘密情報）にて復号をし、復号によって得られる情報が、前記第一の情報と適合しているかを判断することになる。これを本発明に応用した場合、機器Ａはアプリ実行手段３３に、また、機器Ｂがカードアプリ１１に相当するが、機器Ａは秘密情報Ａに相当するデータをセキュアに保持しておく領域を有しないため、秘密情報Ａに替えてアプリ実行手段３３が生成したダイジェストデータを、また、秘密情報Ｂに替えてセキュアデバイスがあらかじめ保持しているダイジェストデータ１５をそれぞれ用いることで可能となる。

【００３４】

（第３の実施形態）

本発明の第３の実施形態では、携帯端末の中でセキュアデバイスの信頼性を得たアプリ実行手段が、電子署名付きのアプリを認証し、この認証結果をセキュアデバイスが受け入れるアプリケーション認証システムについて説明する。

図６は、このシステムを構成するセキュアデバイス１０と携帯端末３０とを模式的に示している。セキュアデバイス１０は、署名検証用ルート証明書を有していない。その他の構成は、第１の実施形態と変わりが無い。

【００３５】

図５には、このシステムにおける認証手順を矢印で示している。

セキュアデバイス１０が携帯端末３０に装着されると、第１の実施形態（図１）と同様に、セキュアデバイス１０のカードマネージャ１３と、携帯端末３０のＪＡＭ３３との間で、装置間の相互認証処理が行われ（１）、相互認証に成功すると、カードマネージャ１３は、その成功を示す相互認証パスフラグをセキュアデバイス１０内に立てる。また、携帯端末３０のＪＡＭ３３は、セキュアデバイス１０との相互認証に成功すると、セキュアデバイス１０へのアクセス機能を開始し、Java(登録商標)アプリ３１は、ＪＡＭ３３に対してセキュアデバイス１０へのアクセスを要求する（２－１）。この要求を受けたＪＡＭ３３は、アプリ証

明書に含まれる公開鍵を用いてJava(登録商標)アプリ３１の電子署名３４を検証し、それによりJava(登録商標)アプリ３１を認証する（２－２）。このＪＡＭ３３によるJava(登録商標)アプリ３１の認証処理は、第１の実施形態で説明したものと同じである。

【００３６】

Java(登録商標)アプリ３１を認証したＪＡＭ３３は、Java(登録商標)アプリ３１からのアクセス要求を実行し、カードアプリ１１にコマンドを送信する（３）。セキュアデバイス１０のカードアプリ１１は、カードマネージャ１３による機器認証が完了していることを相互認証パスフラグで確認した後、このコマンドを受け付ける。

このように、このアプリケーション認証システムのセキュアデバイスは、携帯端末との相互認証で、携帯端末の書き換え不可領域に格納されたJava(登録商標)実行環境（アプリ実行手段）を認証すると、このアプリ実行手段により行われた、電子署名付きアプリの認証結果を信用して、このアプリを認証する。

【００３７】

このアプリケーション認証システムでは、アプリに署名を付ける方式を規定している既存方式（Ｊ２ＳＥなど）がそのまま利用可能であり、また、こうした方式を用いてアプリへ署名を付けているシステムは、この実施形態のシステムに、障害無く移行することができる。

また、このシステムでは、第２の実施形態の場合とは逆に、アプリへの署名付けの権利を持つオペレータなどの主体は、ビジネスをコントロールすることができる。

【００３８】

なお、セキュアデバイスには、各実施形態で示したように、格納されているデータへのアクセスをカードアプリが制御するプログラムアプリ型のデバイスと、格納したファイルにアクセスするためのセキュリティ条件を決めるファイルアプリ型のデバイスとがある。後者のセキュアデバイスでは、図７に示すように、Java(登録商標)実行環境がカードマネージャの認証をパスした場合に、Java(登録商標)実行環境が選択するＤＦ（Dedicated File）の傘下のＥＦ（Elementary Fi

le）へのアクセスが可能になり、また、各実施形態の方式でアプリが認証された場合に、そのアプリが選択するＤＦの傘下のＥＦへのアクセスが可能になるようにセキュリティ条件を設定することができる。

【００３９】

なお、セキュアデバイスがアプリ実行手段を認証した後でも、セキュアデバイスにおける端末への装着部にある端子から、悪意のある人間によって、アプリ実行手段になりすましてあたかもアプリ実行手段からの信号であるかのようにセキュアデバイスに指示を送ることも不可能とは言い切れなく、そのような場合、このなりすましを防ぐためには、確かにアプリ実行手段からの指示であることを確認できる工夫があると更に好ましい。その工夫としては次のようなものが考えられる。

【００４０】

つまり、カードマネージャ１３がアプリ実行手段３３を認証する処理（１）にて、カードマネージャ１３からアプリ実行手段３３へ任意の情報を送信して両者で共有するか、両者に共通の情報が保持されている（あるいは生成する）場合はその情報を記憶しておく。この情報を第二の情報とすると、アプリ実行手段３３からカードアプリ１１へアクセス要求を行う処理（３）にて、前記第二の情報も加味する。カードアプリ１１では、受信したアクセス要求に第二の情報が加味されている要求のみを受付、加味されていなければなりすましなど不正なアクセスとみなしその処理を受け付けない。なお、ここで「第二の情報を加味」とは、アクセス要求に第二の情報を付加したり、アクセス要求の全部または一部の情報を、そのまま乃至加工したものを暗号化したりすることなどを意味する。

【００４１】

【発明の効果】

以上の説明から明らかなように、本発明のアプリケーション認証システムでは、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。そのため、端末上のアプリは、端末に装着されたセキュアデバイスのデータへのアクセスが可能になり、高度な処理を実行することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態におけるアプリケーション認証システムの手順を示す図

【図２】

本発明の第１の実施形態におけるアプリケーション認証システムの構成を示す図

【図３】

本発明の第２の実施形態におけるアプリケーション認証システムの手順を示す図

【図４】

本発明の第２の実施形態におけるアプリケーション認証システムの構成を示す図

【図５】

本発明の第３の実施形態におけるアプリケーション認証システムの手順を示す図

【図６】

本発明の第３の実施形態におけるアプリケーション認証システムの構成を示す図

【図７】

本発明の実施形態におけるファイルアプリ型セキュアデバイスでのファイルアクセスを示す図

【図８】

セキュアデバイスを装着した携帯端末で実現可能なサービスを示す図

【図９】

携帯端末上のアプリをセキュアデバイスが認証するときの問題点を示す図

【符号の説明】

１０　セキュアデバイス

１１　カードアプリ

１３　共通ライブラリ（カードマネージャ）

１４　署名検証用ルート証明書

１５　ダイジェストデータ

３０　携帯端末

３１　Java(登録商標)アプリ

３２　ＯＳ

３３　Java(登録商標)実行環境（ＪＡＭ）

３４　電子署名

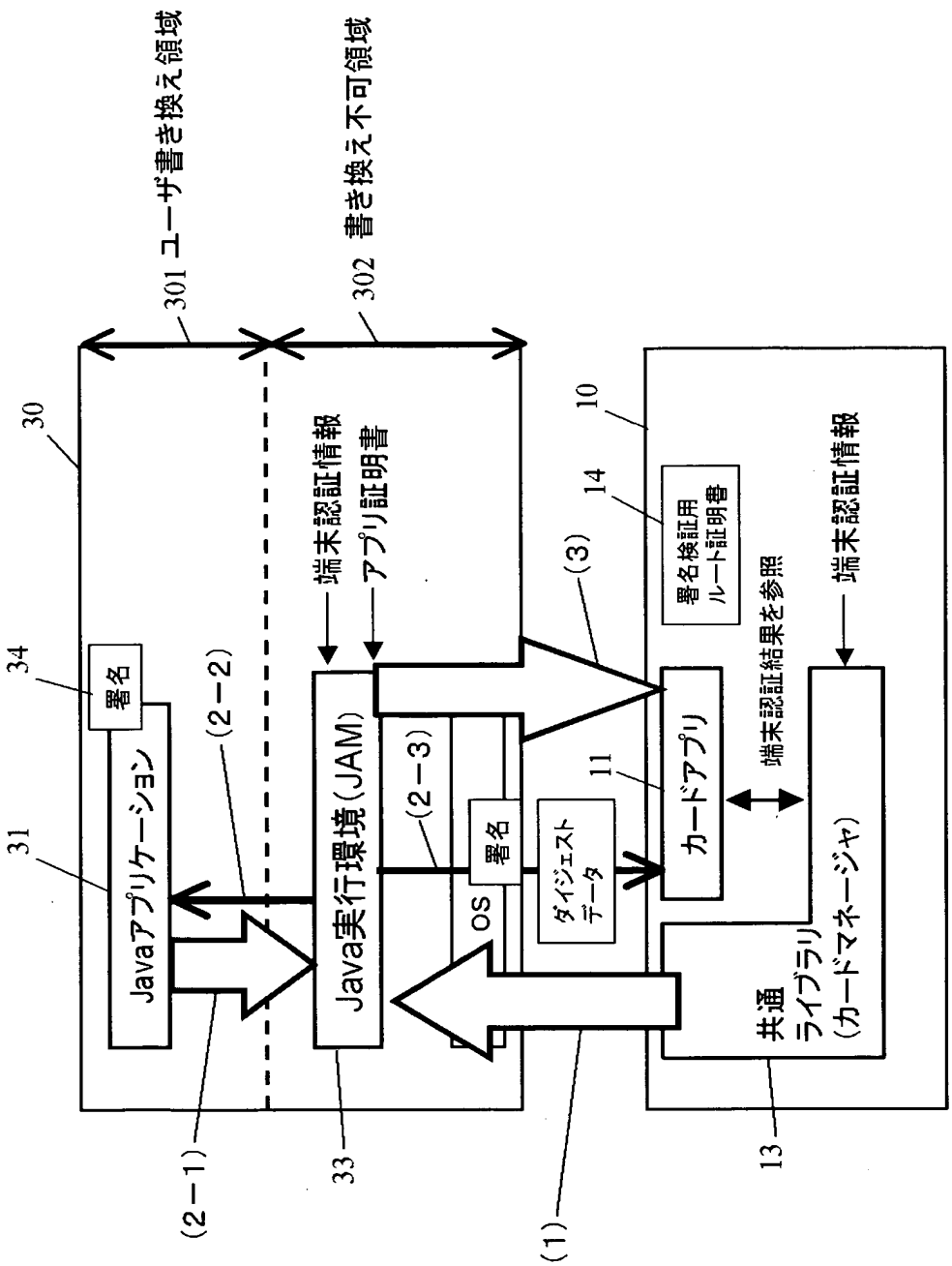
３５　秘密情報格納領域

３０１　ユーザ書き換え領域

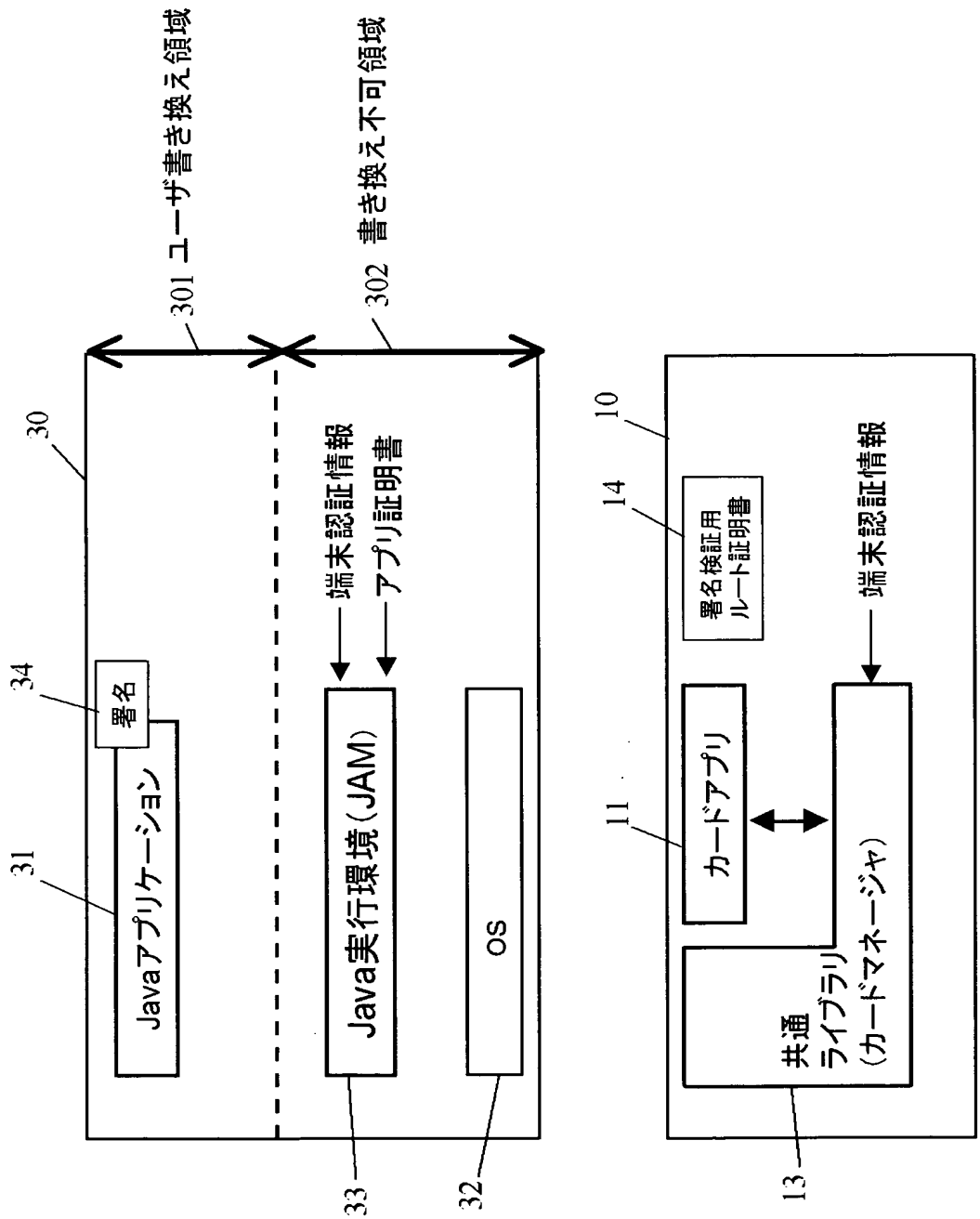
３０２　書き換え不可領域

【書類名】　図面

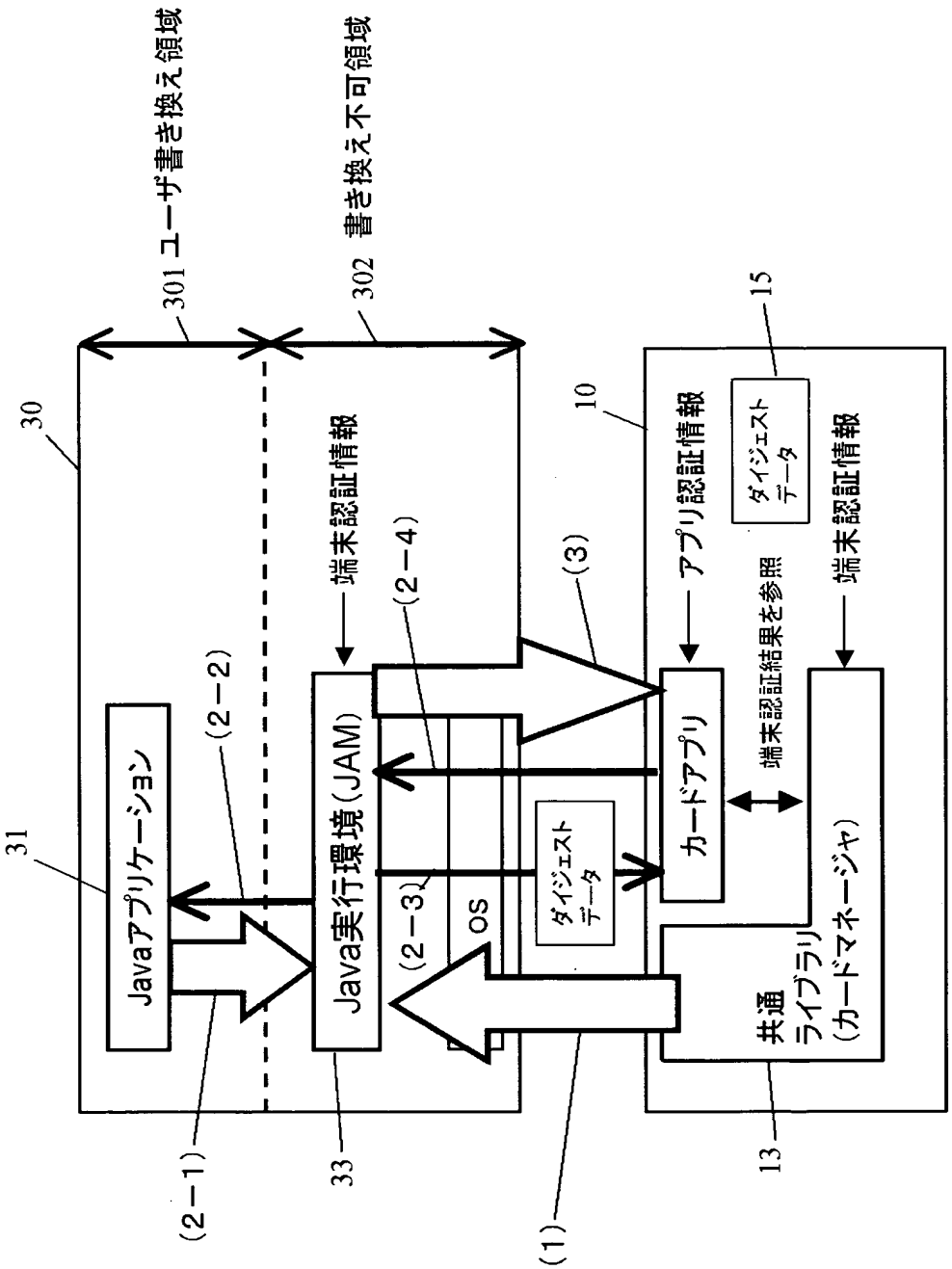
【図１】


301 ユーザ書き換え領域
302 書き換え不可領域
30
34
署名
31
Javaアプリケーション
(2－2)
端末認証情報
アプリ証明書
Java実行環境(JAM)
(2－3)
署名
ダイジェスト
データ
OS
(3)
10
14
署名検証用
ルート証明書
11
カードアプリ
端末認証結果を参照
端末認証情報
共通
ライブラリ
(カードマネージャ)
(2－1)
33
(1)
13

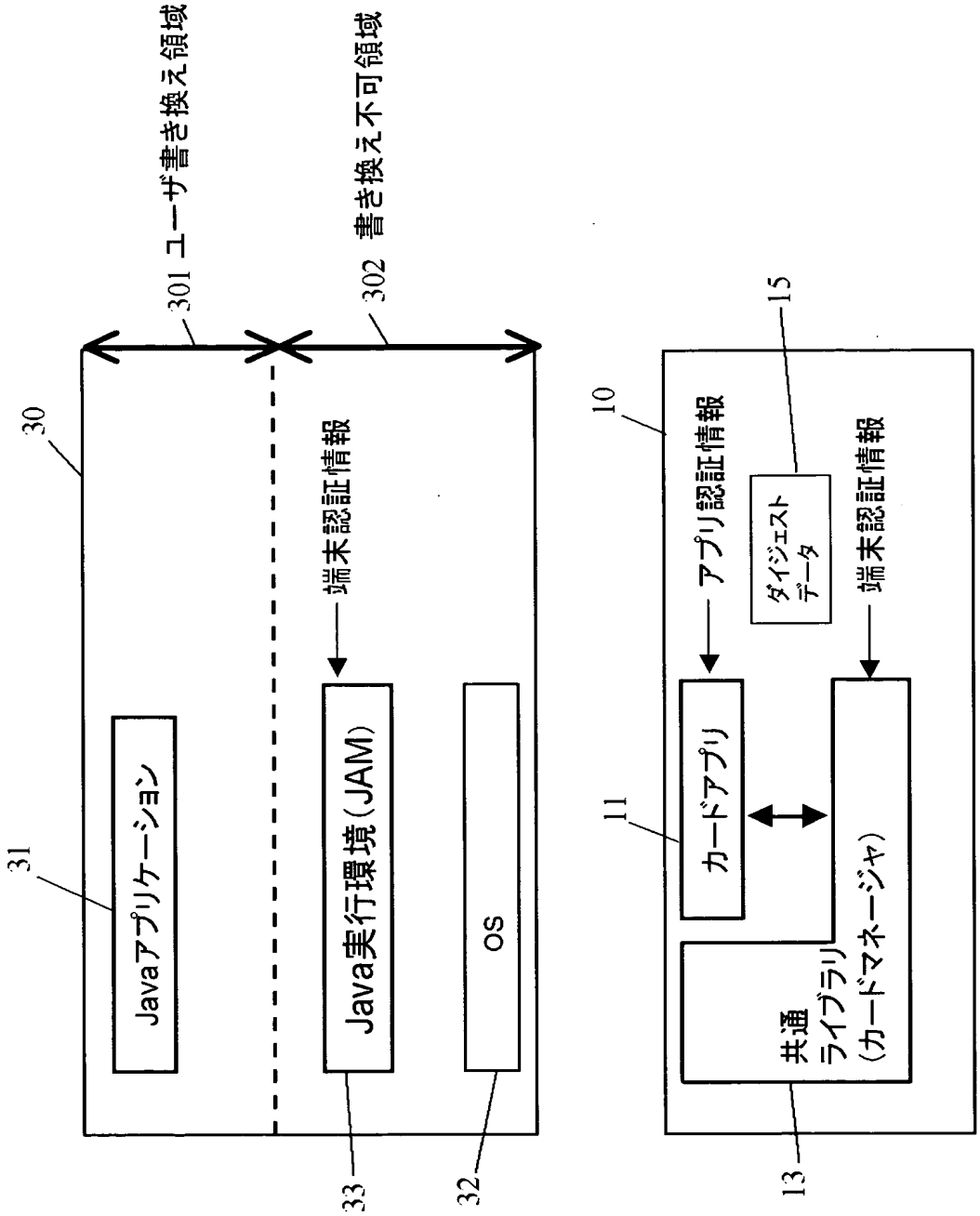
【図２】


301 ユーザ書き換え領域
302 書き換え不可領域
30
34
署名
31
Javaアプリケーション
端末認証情報
アプリ証明書
Java実行環境(JAM)
OS
33
32
10
14
署名検証用
ルート証明書
端末認証情報
11
カードアプリ
共通
ライブラリ
(カードマネージャ)
13

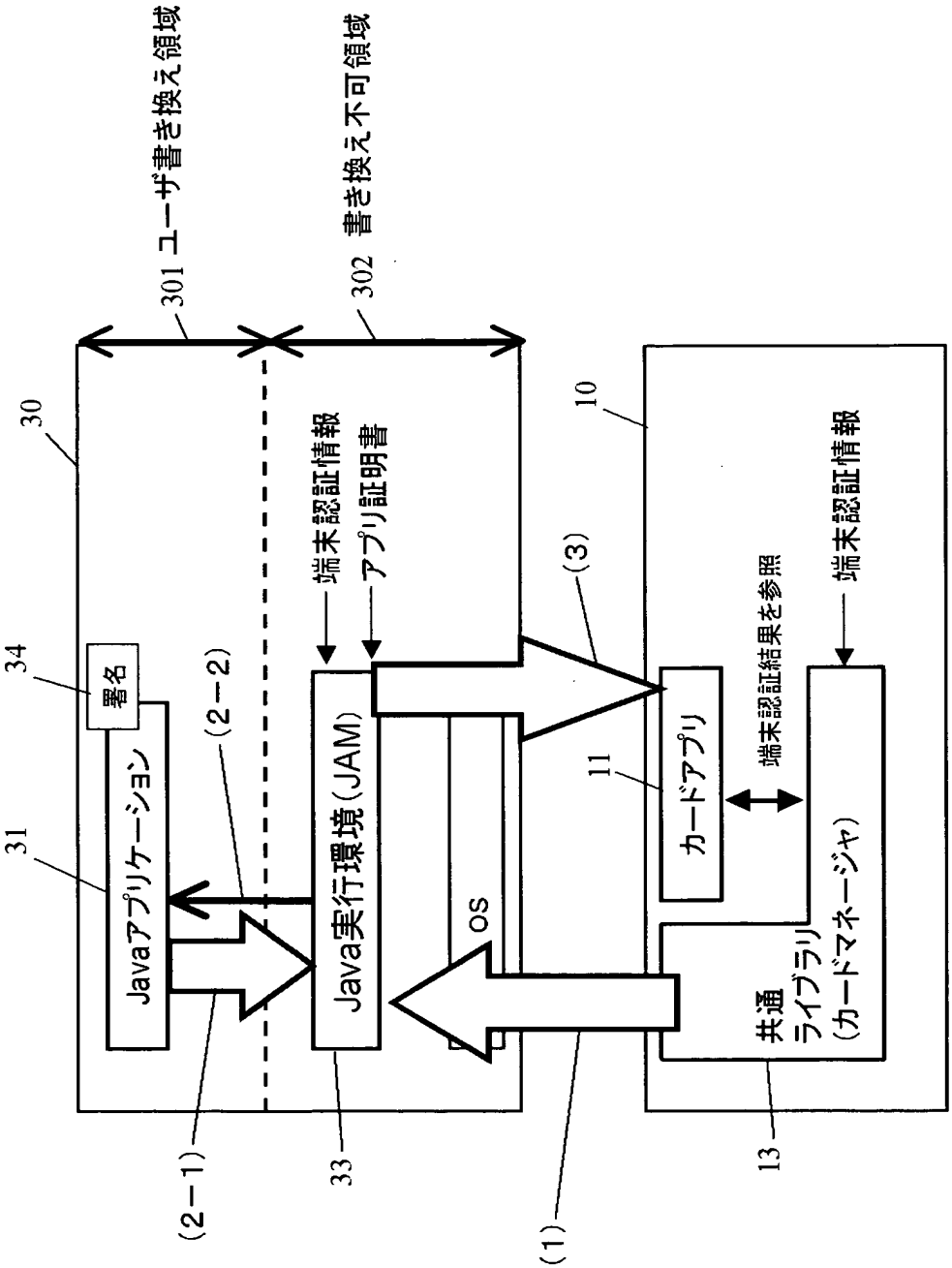
【図３】


301 ユーザ書き換え領域
302 書き換え不可領域
30
31
10
15
Javaアプリケーション
Java実行環境(JAM)
OS
ダイジェストデータ
端末認証情報
アプリ認証情報
ダイジェストデータ
端末認証情報
カードアプリ
端末認証結果を参照
共通ライブラリ(カードマネージャ)
(1)
(2−1)
(2−2)
(2−3)
(2−4)
(3)
33
13

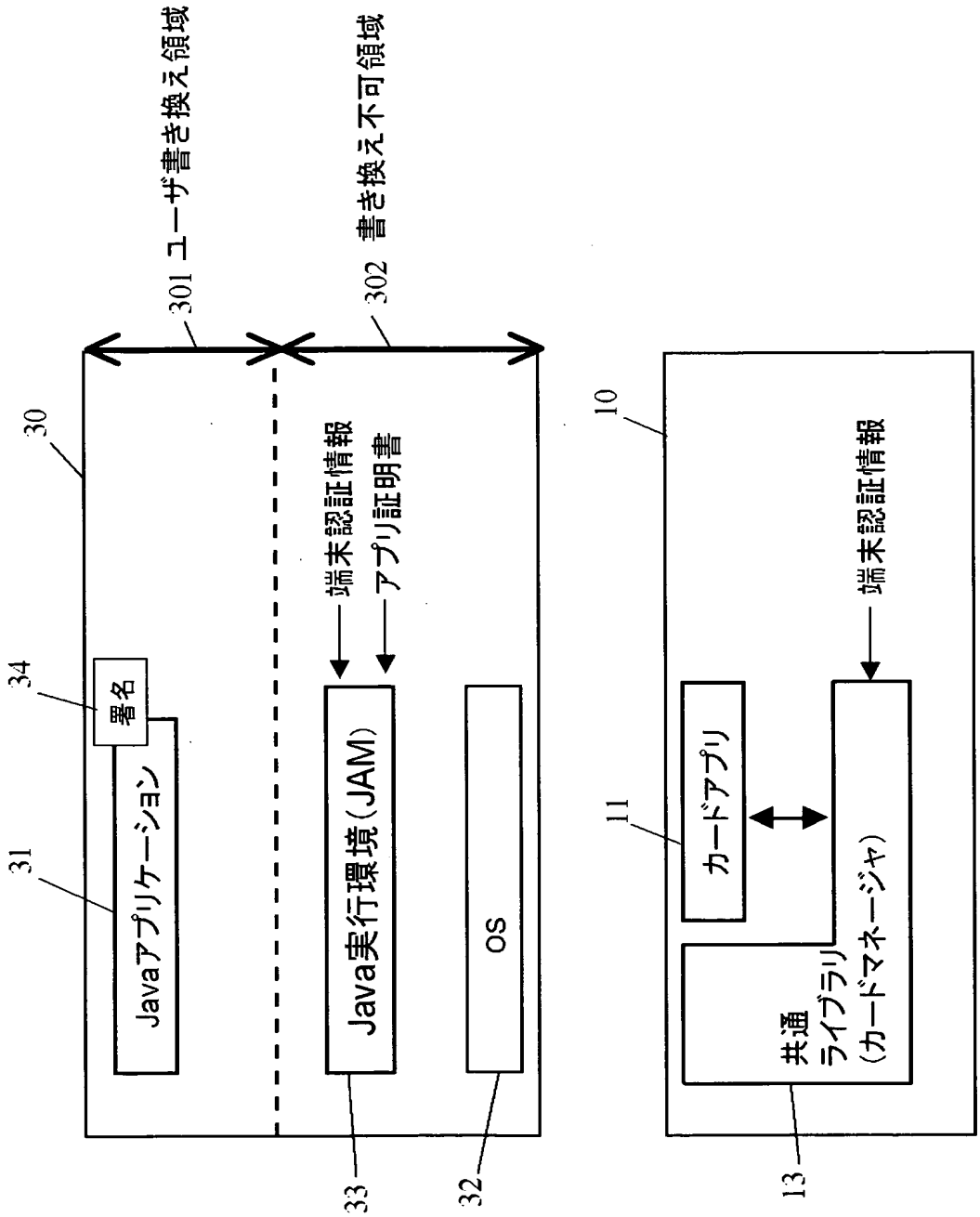
【図４】


301 ユーザ書き換え領域
302 書き換え不可領域
30
31
Javaアプリケーション
Java実行環境（JAM）
OS
端末認証情報
33
32
10
15
アプリ認証情報
ダイジェストデータ
端末認証情報
11
カードアプリ
共通ライブラリ（カードマネージャ）
13

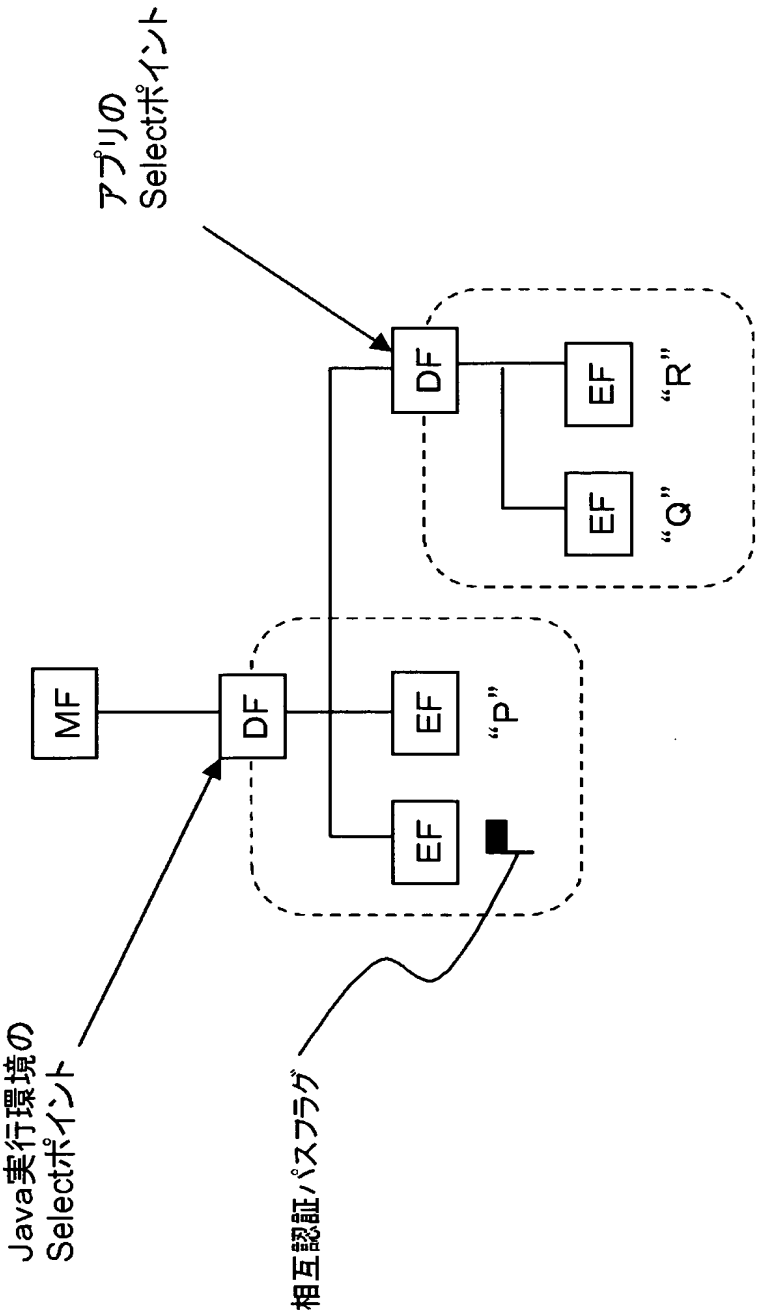
【図５】


301 ユーザ書き換え領域
302 書き換え不可領域
30
10
34
署名
31
Javaアプリケーション
(2－2)
端末認証情報
アプリ証明書
(3)
端末認証情報
11
カードアプリ
端末認証結果を参照
Java実行環境(JAM)
OS
共通
ライブラリ
(カードマネージャ)
(2－1)
33
(1)
13

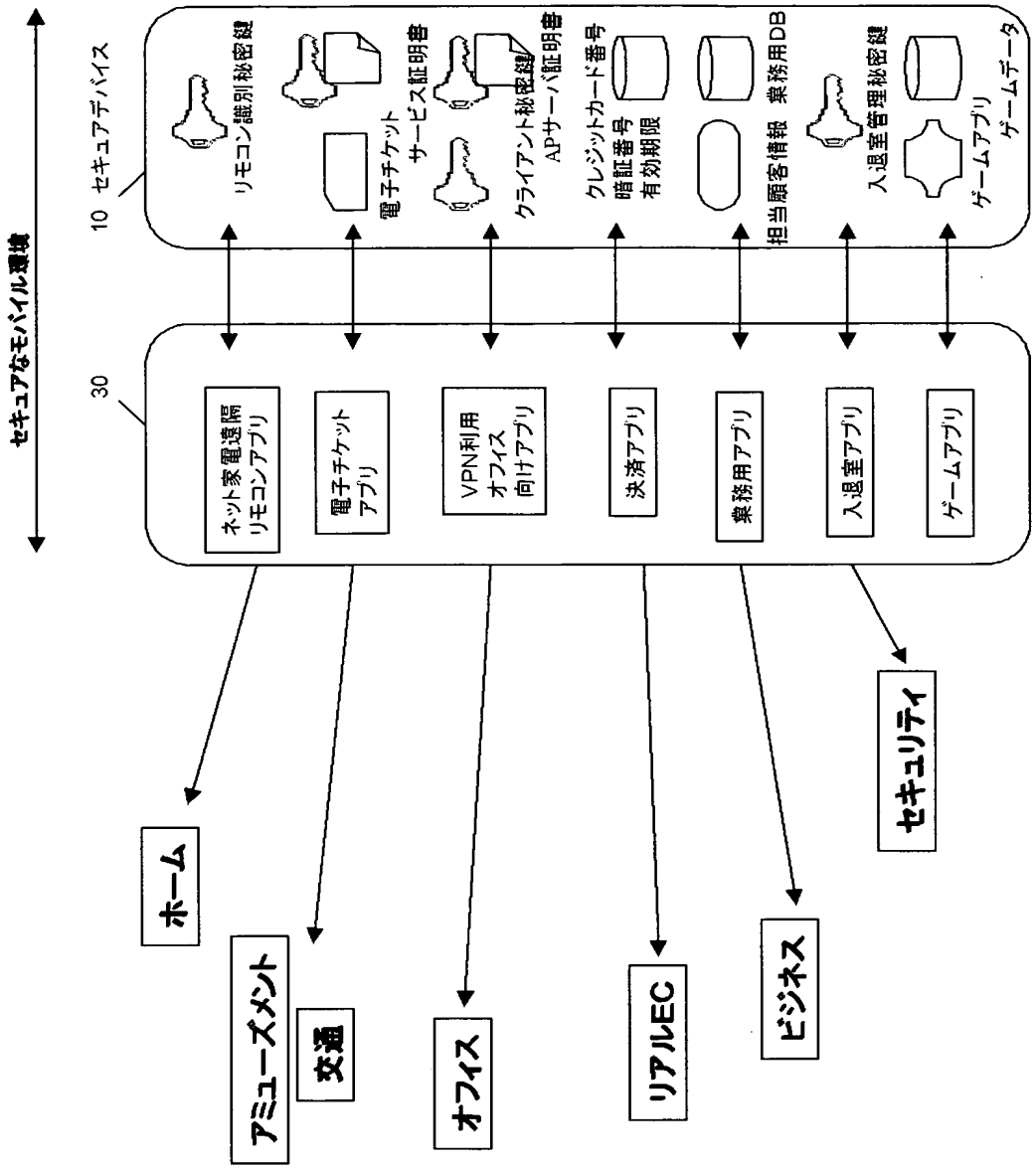
【図６】


301 ユーザ書き換え領域
302 書き換え不可領域
30
34
署名
31
Javaアプリケーション
端末認証情報
アプリ証明書
Java実行環境(JAM)
OS
33
32
10
11
カードアプリ
端末認証情報
共通
ライブラリ
(カードマネージャ)
13

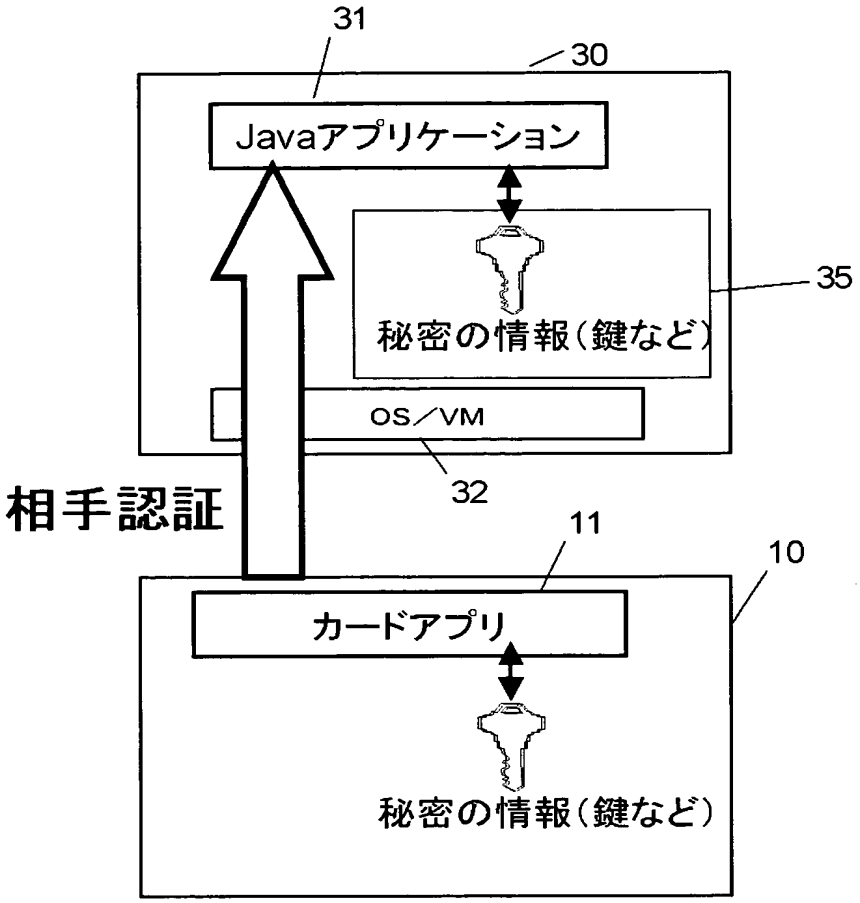
【図７】


アプリの
Selectポイント
DF
EF
"R"
EF
"Q"
MF
DF
EF
"P"
EF
Java実行環境の
Selectポイント
相互認証パスフラグ

【図８】


セキュアなモバイル環境
10 セキュアデバイス
リモコン識別秘密鍵
電子チケット
サービス証明書
クライアント秘密鍵/
APサーバ証明書
クレジットカード番号
暗証番号
有効期限
担当顧客情報 業務用DB
入退室管理秘密鍵
ゲームアプリ
ゲームデータ
30
ネット家電遠隔
リモコンアプリ
電子チケット
アプリ
VPN利用
オフィス
向けアプリ
決済アプリ
業務用アプリ
入退室アプリ
ゲームアプリ
ホーム
アミューズメント
交通
オフィス
リアルEC
ビジネス
セキュリティ

【図９】


31
30
Javaアプリケーション
35
秘密の情報（鍵など）
OS／VM
32
相手認証
11
10
カードアプリ
秘密の情報（鍵など）

【書類名】　　要約書

【要約】

【課題】　安全な情報秘匿領域を持たない端末上のアプリに対するセキュアデバイスの認証が可能なアプリケーション認証システムを提供する。

【解決手段】　安全な情報秘匿領域を持たない端末３０に装着されたセキュアデバイス１０が、端末に格納されたアプリ３１を認証するアプリケーション認証システムにおいて、セキュアデバイス１０が、端末の書き換え不可領域３０２に格納されたアプリ実行手段３３を認証し、このアプリ実行手段が、セキュアデバイスへのアクセスを要求するアプリ３１に対して行った処理に基づいて、アプリを認証するように構成している。セキュアデバイスと端末との相互認証、及び、端末内でのアプリの認証とを結び付けることで、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。

【選択図】　　図１

特願２００３－０５３３６２

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社